

UTILITY PATENT APPLICATION TRANSMITTAL

Only for new nonprovisional applications under 37 CFR 1.53(b)

Attorney Docket No. 35.G2561

First Named Inventor or Application Identifier

KEIICHI IWAMURA

Express Mail Label No.

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

ADDRESS TO:

Assistant Commissioner for Patents
Box Patent Application
Washington, DC 20231

1. ☒ Fee Transmittal Form
(Submit an original, and a duplicate for fee processing)

2. ☒ Specification Total Pages **40**

3. ☒ Drawing(s) (35 USC 113) Total Sheets **7**

4. ☒ Oath or Declaration Total Pages **1**

a. ☐ Newly executed (original or copy)

b. ☒ Unexecuted for information purposes

c. ☐ Copy from a prior application (37 CFR 1.63(d))
(for continuation/divisional with Box 17 completed)
[Note Box 5 below]

☐ **DELETION OF INVENTOR(S)**
Signed Statement attached deleting
inventor(s) named in the prior application, see
37 CFR 1.63(d)(2) and 1.33(b).

☐ Incorporation By Reference (useable if Box 4c is checked)
The entire disclosure of the prior application, from which a copy of
the oath or declaration is supplied under Box 4c, is considered as
being part of the disclosure of the accompanying application and is
hereby incorporated by reference therein.

6. ☐ Microfiche Computer Program (Appendix)

7. Nucleotide and/or Amino Acid Sequence Submission
(if applicable, all necessary)

a. ☐ Computer Readable Copy

b. ☐ Paper Copy (identical to computer copy)

c. ☐ Statement verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

8. ☐ Assignment Papers (cover sheet & document(s))

9. ☐ 37 CFR 3.73(b) Statement ☐ Power of Attorney
(when there is an assignee)

10. ☐ English Translation Document (if applicable)

11. ☐ Information Disclosure ☐ Copies of IDS
Statement (IDS)/PTO-1449 Citations

12. ☐ Preliminary Amendment

13. ☒ Return Receipt Postcard (MPEP 503)
(Should be specifically itemized)

14. ☐ Small Entity ☐ Statement filed in prior application
Statement(s) Status still proper and desired

15. ☐ Certified Copy of Priority Document(s)
(if foreign priority is claimed)

16. ☐ Other: _____

17. If a CONTINUING APPLICATION, check appropriate box and supply the requisite information:

☐ Continuation

☐ Divisional

☐ Continuation-in-part (CIP) of prior application No. _____

18. CORRESPONDENCE ADDRESS

☒ Customer Number or Bar Code Label

05514

(Insert Customer No. or Attach bar code label here)

or ☐ Correspondence address below

NAME

Address

City

Country

State

Telephone

Zip Code

Fax

CLAIMS	(1) FOR	(2) NUMBER FILED	(3) NUMBER EXTRA	(4) RATE	(5) CALCULATIONS
	TOTAL CLAIMS (37 CFR 1.16(c))	33-20 =	13	X \$ 18.00 =	\$ 234.00
	INDEPENDENT CLAIMS (37 cfr 1.16(b))	8-3 =	5	X \$ 78.00 =	\$ 390.00
	MULTIPLE DEPENDENT CLAIMS (if applicable) (37 CFR 1.16(d))			\$ 260.00 =	\$ 0.00
				BASIC FEE (37 CFR 1.16(e))	\$ 690.00
	Total of above Calculations =				\$1314.00
	Reduction by 50% for filing by small entity (Note 37 CFR 1 9, 1 27, 1 28).				
	TOTAL =				\$1314.00

19. Small entity status

- a. ☐ A Small entity statement is enclosed
- b. ☐ A small entity statement was filed in the prior nonprovisional application and such status is still proper and desired.
- c. ☐ Is no longer claimed.

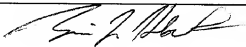
20. ☒ A check in the amount of \$ 1314.00 to cover the filing fee is enclosed.

21. ☐ A check in the amount of \$ _____ to cover the recordal fee is enclosed.

22. The Commissioner is hereby authorized to credit overpayments or charge the following fees to Deposit Account No. 06-1205:

- a. ☒ Fees required under 37 CFR 1.16.
- b. ☐ Fees required under 37 CFR 1.17.
- c. ☐ Fees required under 37 CFR 1.18.

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

NAME	Brian L. Klock - Reg. No. 36,570
SIGNATURE	
DATE	March 29, 2000

BLKlcmv

TITLE OF THE INVENTION

INFORMATION PROCESSING SYSTEM, INFORMATION PROCESSING
APPARATUS, AND COMPUTER-READABLE RECORDING MEDIUM

5

BACKGROUND OF THE INVENTION

Field of the Invention

0537377-025000
10 The present invention relates to information processing
systems, information processing apparatuses, and computer-
readable recording media used in the systems or the
apparatuses, suited to cases in which electronic-watermark
information is embedded in input information, such as
digital image data or digital sound data, to protect
copyright, to prevent forgery, and to record various types
15 of information.

Description of the Related Art

20 As computers and networks have been remarkably
developed in recent years, various types of information,
such as character data, image data, and sound data, has been
handled in the computers and networks. Since such data is
digital, it can be easily copied with its quality maintained.
Therefore, to protect the copyright of such data, copyright
information and user information are embedded in image data
and sound data as electronic-watermark information
25 (hereinafter just called an electronic watermark) in many

cases.

With the use of an electronic-watermark technology, information which people cannot recognize with their senses of sight and hearing is confidentially embedded in image data or sound data. When an embedded electronic watermark is extracted from image data or sound data, copyright information, user information, and identification information are obtained, and illegitimate copying can be traced.

10 A first condition required for such an electronic watermark is a quality at which embedded information cannot be identified, namely, at which information is embedded in the original digital information such that the quality of the original digital information does not deteriorate.

15 A second condition is robustness with which information embedded in the original digital information remains, namely, with which embedded information is not lost even if editing, such as data compression and filtering, or an attack is applied.

20 A third condition is the amount of information to be embedded, which can be selected according to use.

These conditions, required for electronic watermarks, are generally tradeoffs to each other. When an electronic watermark having a high robustness is generated, for example, 25 relatively large quality deterioration occurs and the amount

00537077.000000

of information to be embedded becomes small in many cases.

Methods for embedding electronic watermarks in multi-valued still pictures can be divided into two types, spatial-domain embedding methods and frequency-domain embedding methods.

In each of various electronic-watermark embedding methods, embedding processing corresponds to extracting processing one by one, and there are no compatibility. In general, it is said that spatial-domain embedding methods provide a low quality deterioration with a low robustness, whereas frequency-domain embedding methods provide a high robustness with a relatively high quality deterioration. Each method has a different feature, such as a high robustness with a small amount of embedded information, or a high quality with a low robustness.

To protect embedded information, information (hereinafter called a key) indicating algorithm, embedding positions, and changes are kept confidential in many cases. This is to enhance robustness to an intentional attack in which the algorithm and embedding positions are analyzed to remove electronic watermarks.

It can be considered to efficiently protect copyright that a monitoring organization for checking whether illegitimate copying is performed, by extracting electronic watermarks is provided. It is important for such a

monitoring organization to keep the electronic-watermark method used and the key confidential to avoid an intentional attack.

As described above, there are various electronic-watermark methods each having its features. There are also many companies and associations which want to prevent illegitimate copying and illegitimate outputting of digital data by the use of electronic watermarks. If such companies and associations independently select electronic-watermark methods to embed electronic watermarks in data, since embedding processing and extracting processing correspond one by one in each of electronic-watermark methods and they are not compatible, the following problems occur.

1. It is difficult for one monitoring organization to perform united checking because electronic-watermark extracting processing is needed for each method.

2. To perform united checking by one monitoring organization, the monitoring organization needs to have all electronic-watermark extracting techniques, causing a large load.

3. The monitoring organization needs to manage the keys corresponding to all the extracting techniques confidentially and strictly.

4. When a monitoring organization is provided for each method, if an embedded electronic watermark cannot be

extracted, it cannot be determined whether the embedded electronic watermark has been generated by a different method, or the electronic watermark is broken by an attack.

One monitoring organization refers to one configuration
5 in terms of a system or a method, determined by standardization or a nation, rather than one physical organization.

SUMMARY OF THE INVENTION

10 Accordingly, it is an object of the present invention to efficiently protect copyrighted materials in various electronic-watermark methods.

15 The foregoing object is achieved in one aspect of the present invention through the provision of an information processing system in which a plurality of information processing apparatuses are connected through a network, at least one of the plurality of information processing apparatuses including first adding means for adding first
20 additional information to input information by a first adding method; and second adding means for adding second additional information to the input information by a second adding method, wherein the first adding method has a higher robustness than the second adding method.

25 The foregoing object is achieved in another aspect of the present invention through the provision of an

information processing system in which a plurality of information processing apparatuses are connected through a network, at least one of the plurality of information processing apparatuses including first extracting means for
5 extracting first additional information from input information by a first extracting method; and second extracting means for extracting second additional information from the input information by a second extracting method identified by the extracted first
10 additional information.

0557877-032900
15 The foregoing object is achieved in still another aspect of the present invention through the provision of an information processing apparatus including first adding means for adding first additional information to input information at a high robustness by a first adding method; and second adding means for adding second additional information to the input information by a second adding method.

20 The foregoing object is achieved in yet another aspect of the present invention through the provision of an information processing apparatus including first extracting means for extracting first additional information from input information by a first extracting method; and second
25 extracting means for extracting second additional information from the input information by a second

extracting method identified by the extracted first additional information.

The foregoing object is achieved in still yet another aspect of the present invention through the provision of an information processing method including a first adding step of adding first additional information to input information at a high robustness by a first adding method; and a second adding step of adding second additional information to the input information by a second adding method.

0537877.032900
10 The foregoing object is achieved in a further aspect of the present invention through the provision of an information processing method including a first extracting step of extracting first additional information from input information by a first extracting method; and a second
15 extracting step of extracting second additional information from the input information by a second extracting method.

The foregoing object is achieved in a still further aspect of the present invention through the provision of a computer-readable recording medium for storing a program,
20 the program including a first adding step of adding first additional information to input information at a high robustness; and a second adding step of adding second additional information to the input information.

The foregoing object is achieved in a yet further
25 aspect of the present invention through the provision of a

computer-readable recording medium for storing a program,
the program including a first extracting step of extracting
first additional information from input information; an
identifying step of identifying an extracting method by the
5 extracted first additional information; and a second
extracting step of extracting second additional information
from the input information by the identified extracting
method.

Other objects and other features of the present
10 invention will become clear by the following figures and
descriptions.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram of a portion related to
15 electronic-watermark embedding in an information processing
system according to a first embodiment of the present
invention.

Fig. 2 is a block diagram of a portion related to
electronic-watermark extracting in the information
20 processing system according to the first embodiment of the
present invention.

Fig. 3 is a block diagram of a portion related to
electronic-watermark embedding in an information processing
system according to a second embodiment of the present
25 invention.

Fig. 4 is a block diagram of a portion related to electronic-watermark extracting in the information processing system according to the second embodiment of the present invention.

5 Fig. 5 is a block diagram of a portion related to electronic-watermark extracting in an information processing system according to a third embodiment of the present invention.

10 Fig. 6 is a block diagram of a portion related to electronic-watermark embedding and extracting in an information processing system according to a fourth embodiment of the present invention.

15 Figs. 7A and 7B are block diagrams of an electronic-watermark embedding apparatus and an electronic-watermark extracting apparatus, respectively.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

(First embodiment)

20 Fig. 1 shows a portion related to electronic-watermark embedding in an information processing system according to a first embodiment of the present invention. This system uses a common electronic-watermark method and electronic-watermark methods unique to monitoring organizations. The common electronic-watermark method refers to an electronic-watermark method determined by standardization or related

25

organizations, and the features thereof will be described later.

In Fig. 1, organizations 101 to 104 perform electronic-watermark embedding processing with the use of different electronic-watermark methods. In the organizations 101 to 104, common-electronic-watermark embedding apparatuses 105 perform electronic-watermark embedding processing by the predetermined common electronic-watermark method, and a type-A-electronic-watermark embedding apparatus 106, a type-B-electronic-watermark embedding apparatus 107, a type-C-electronic-watermark embedding apparatus 108, and type-D-electronic-watermark embedding apparatus 109 perform electronic-watermark embedding by electronic-watermark methods independently determined by the organizations 101 to 104, respectively. A network 110 connect the organizations. The organizations 101 to 104 have communication means, not shown, for connecting to the network 110.

The common electronic-watermark method, which the common-electronic-watermark embedding apparatus 105 uses, has the following features.

1. Implements high-robustness electronic watermarks with a relatively small amount of information.
2. Extracts electronic watermarks without keys or with a common key.
3. Embeds information which identifies at least each

electronic-watermark method or the organization which has performed embedding by the use of the method.

4. Has robustness to electronic-watermark embedding performed by each organization.

5 5. Sets a variable level of robustness in steps or continuously by the decision of each organization and attaches data indicating a robustness strength to information in which electronic watermarks are embedded, as additional information.

10 Various electronic-watermark methods having the foregoing methods can be considered. A method having a high robustness will be taken below as example.

15 Fig. 7A shows an electronic-watermark embedding apparatus for performing the above-described embedding processing, and Fig. 7B shows an electronic-watermark extracting apparatus for performing the above-described extracting.

20 When a still picture is input as input data serving as a copyrighted material, the image data of the still picture is divided into eight-by-eight-pixel blocks and discrete cosine transform (DCT) is applied to each block. Hereinafter, a DCT-transformed block is called a DCT coefficient block, one coefficient in a DCT coefficient block is called a DCT coefficient, and a set of DCT
25 coefficient blocks for one sheet of picture is called a DCT

coefficient block group.

In the electronic-watermark embedding apparatus shown in Fig. 7A, an image transform unit 701 applies DCT to an input image "x" and the output of the image transform unit

701, a DCT coefficient block group, is input to an electronic-watermark embedding unit 702. The electronic-watermark embedding unit 702 selects one DCT coefficient block to be embedded among the input DCT coefficient block group, and quantizes one DCT coefficient in the DCT coefficient block to embed one embedding bit.

The size of a quantization step corresponds to the intensity of embedding, and the size of the quantization step and the position of the selected DCT coefficient correspond to key information.

As an example, the value of a DCT coefficient located at the coordinates "u" and "v" is called $s\{u, v\}$, a quantization step is called "h," and an electronic-watermark bit of 0 or 1 is embedded by the following rule.

$$ah < s\{u, v\} \leq (a + 1)h \quad (1)$$

The following operation is executed, and a coefficient used after embedding is set to $c\{u, v\}$.

$$c\{u, v\} = bh + h/2 \text{ for an embedding bit of 0} \quad (2)$$

where b is whichever of "a" and $(a + 1)$ is even.

$$c\{u, v\} = bh + h/2 \text{ for an embedding bit of 1} \quad (3)$$

where b is whichever of "a" and $(a + 1)$ is odd.

Lastly, an inverse-image-transform unit 703 applies inverse DCT to the block group to change it back to eight-by-eight-pixel blocks and reconstructs them. Then, an image "y" in which the electronic watermark has been embedded is
5 obtained.

In the present embodiment, a setting unit 706 for variably setting the size of a quantization step and/or an embedding position to variably specify a robustness strength is provided. This setting unit sets the above factors
10 according to various parameters such as a security level, automatically or by a manual operation of a person who monitors.

Data indicating the specified robustness strength is attached to the original data as additional information at a
15 subsequent stage of the inverse-image-transform unit 703. According to this data, an extracting operation is specified at an extracting side.

The additional information may be common among the organizations, or may be encrypted so that a third party
20 cannot obtain the robustness strength.

To extract the electronic watermark in the electronic-watermark extracting unit shown in Fig. 7B, the image "y" is input to an image transform unit 701, an electronic-watermark extracting unit 705 selects a DCT coefficient
25 which has been embedded with key information among a DCT

coefficient block group to which the same DCT is applied,
"b" which satisfies the following expression is obtained,
when "b" is even, it is determined that the embedding bit is
0, and when "b" is odd, it is determined that the embedding
5 bit is 1.

$$bh < c(u, v) \leq (b + 1)h \quad (4)$$

A method for enhancing the robustness in this embedding
method will be described below.

When a DCT coefficient indicating a low-frequency
10 component is selected from a DCT coefficient block as a DCT
coefficient to be embedded, the robustness is made strong.
This is because, whereas high-frequency components are
likely to be lost due to image compression or various types
of filtering processing, low-frequency components are
15 unlikely to be lost.

In the above embedding method, one DCT coefficient
block is selected and one DCT coefficient is embedded. The
number of DCT coefficient blocks to be selected and the
number of DCT coefficients to be embedded can be increased
20 to enhance the robustness. When only one DCT coefficient is
embedded for one bit, it is highly possible that the value
of the bit is lost due to image compression and various
types of filtering processing. When the identical bits are
embedded in a plurality of DCT coefficients, it is not
25 highly possible that most of them are lost.

00537877.000000

10 The robustness can be enhanced by applying error-
correcting encoding to bits to be embedded themselves. This
is because, even if some of the embedded bits are lost, they
are recovered by an error-correcting code. It is clear that
5 the robustness becomes stronger when the used error-
correcting code has a higher error-correcting capability.
Although the above techniques enhance the robustness, they
may change low-frequency components of an image, or the
quality of the image may deteriorate since many bits are
embedded. Since identical bits are embedded with the use of
many DCT coefficients, a small number of bits are embedded
in many cases. If an inverse operation is performed, the
robustness becomes weaker, but image quality is satisfactory
and a large amount of information can be embedded in an
15 electronic-watermark method.

The robustness-strength setting unit 706 may change the
robustness strength by shifting an embedding position from a
high-frequency side to a low-frequency side, or by changing
the number of items to be embedded.

20 The above-described techniques for enhancing the
robustness have the same tendency not only for methods
employing DCT but also for methods employing wavelet
transform or Fourier transform and methods for directly
manipulating the luminance of a pixel.

25 An embedding procedure will be described below by

referring to Fig. 1. For simplicity, 00, 01, 10, and 11 are embedded by the common electronic-watermark method, which are two-bit information for identifying the organizations 101 to 104. It is clear that other types of information can be embedded.

Each of the organizations 101 to 104 embeds the bit corresponding to each organization in distributed data by the common electronic-watermark method which has the above-described features 1 to 5 and has a high robustness with the use of the common-electronic-watermark embedding apparatus 105. Then, other types of information is embedded with the use of the type-A to type-D electronic-watermark embedding apparatuses 106 to 109 unique to the organizations. When the common electronic-watermark method does not interfere with an electronic-watermark method unique to an organization, namely, when electronic-watermark embedding processing does not affect the common electronic-watermark information, the embedding order can be reversed. In each organization, a different piece of information may be embedded. Alternatively, the same information may be embedded. Each organization can embed various types of information, such as copyright information, user information, and identification information.

Fig. 2 shows a portion related to electronic-watermark extracting in the first embodiment.

In Fig. 2, there are provided a united monitoring organization 200, and electronic-watermark monitoring organizations 201 to 204 corresponding to the organizations 101 to 104 shown in Fig. 1, respectively. The united monitoring organization 200 has a common-electronic-watermark extracting apparatus 205 corresponding to the common-electronic-watermark embedding apparatus 105, and the organizations 201 to 204 include a type-A-electronic-watermark extracting apparatus 206, a type-B-electronic-watermark extracting apparatus 207, a type-C-electronic-watermark extracting apparatus 208, and a type-D-electronic-watermark extracting apparatus 209 corresponding to the type-A to type-D electronic-watermark embedding apparatuses 106 to 109 shown in Fig. 1, respectively. A network 210 connects the organizations 201 to 204. The organizations 201 to 204 have communication means, not shown, for connecting to the network 210. The network 210 may be identical with the network 110 shown in Fig. 1.

An electronic-watermark extracting procedure to be executed in Fig. 2 will be described below.

The united monitoring organization 200 monitors data distributed or used in the network 210. If data which seems to be an illegitimate copy is found or reported on the network, the monitoring organization 200 extracts information embedded by the common electronic-watermark

method, by the use of the common-electronic-watermark
extracting apparatus 205. With this operation, the
organization which embedded the information or the used
method is identified, and the data is sent to the identified
5 organization.

The organization which receives the data extracts
various types of embedded information, by the use of the
electronic-watermark extracting apparatus thereof, which is
either of the type-A to type-D electronic-watermark
10 extracting apparatuses 206 to 209.

According to the present embodiment, even in a system
which uses different electronic-watermark methods in a mixed
way, each organization only needs to manage an embedding
section and an extracting section for its own electronic-
15 watermark method, without preparing embedding sections and
extracting sections for many electronic-watermark methods.
Illegitimate copying is efficiently monitored.

Even when an electronic watermark is not found, safety
is enhanced for the following reasons. If electronic-
20 watermark information is not found, it is difficult to
differentiate among whether the data does not include
electronic-watermark information from the beginning, whether
an electronic watermark has been embedded by another method,
and whether electronic-watermark information is broken by an
25 attack. Since the common electronic-watermark method has a

high robustness, it is difficult for an attack to break electronic-watermark information generated by the method.

Therefore, when electronic-watermark information generated by the common electronic-watermark method is extracted in a first process, a possibility of not having electronic-watermark information from the beginning is eliminated. An electronic-watermark method unique to each organization may be used. When detailed information is embedded, a large amount of information is embedded and an electronic-watermark method having a relatively low robustness with suppression of quality deterioration being focused on is used in many cases. Therefore, after electronic-watermark information generated by the common electronic-watermark method is extracted, when electronic-watermark information generated by the electronic-watermark method unique to each organization is not found, it can be said that electronic-watermark information has been broken by an attack.

Therefore, overall safety has been improved by this system, as compared with a case in which each organization independently uses a unique electronic-watermark method.

In the present embodiment, four organizations are included. It is clear that the present invention can also be applied in the same way to a system having any number of organizations.

(Second embodiment)

Fig. 3 shows a portion related to electronic-watermark embedding in an information processing system according to a second embodiment of the present invention. In the present
5 embodiment, only a common-electronic-watermark embedding organization 300 uses the common electronic-watermark embedding apparatus 105 for embedding.

Organizations 301 to 304 only have the type-A to type-D electronic-watermark embedding apparatuses 106 to 109, which
10 use the unique electronic-watermark methods. The organizations 301 to 304 are formed by removing the common-electronic-watermark embedding apparatuses 105 from the organizations 101 to 104 shown in Fig. 1. A network 110 connects the organizations 301 to 304.

15 A united copyright management organization, such as Japanese Society for Right of Authors, Composers and Publishers (JASRAC) for musical copyrighted materials, can serve as the common-electronic-watermark embedding organization 300. Sales shops which sell the users
20 copyrighted materials controlled by the common-electronic-watermark embedding organization 300 can serve as the organizations 301 to 304. The present embodiment does not limit cases to which the present invention is applied. The
25 present invention includes all techniques in which the common-electronic-watermark method having a high robustness

and an electronic-watermark method unique to each organization are used according to conditions.

The organizations 301 to 304 (including each copyright holder) register copyrighted materials at the organization 300 and ask it to execute embedding with the use of the common-electronic-watermark embedding apparatus 105. The organization 300 embeds predetermined information by the common electronic-watermark method, and sends back data to the organizations 301 to 304. The organizations 301 to 304 use the type-A to type-D embedding apparatuses 106 to 109, which employ the unique electronic-watermark methods, to embed various types of information.

The present embodiment has the following advantages over the first embodiment.

In the first embodiment, since each organization performs embedding by the common electronic-watermark method, the common electronic-watermark method and its key need to be made public to each organization. It is better to keep the common electronic-watermark method and its key confidential for safety. If even one organization leaks information, the entire safety cannot be maintained. In the present embodiment, however, since the common electronic-watermark method does not need to be made public to the organizations 301 to 304, safety is enhanced.

The present embodiment can be combined with the first

embodiment. When, in Fig. 3, the organizations 301 and 302 have the common electronic-watermark embedding apparatuses 105 in the same way as in the first embodiment, for example, the organizations 303 and 304, which do not have the common electronic-watermark apparatus 105, performs the same processing as in the present embodiment, and the organizations 301 and 302, which have the common electronic-watermark apparatuses 105, can embed the predetermined information by the common electronic-watermark method within their organizations, as in the first embodiment.

Fig. 4 shows a portion related to electronic-watermark extracting in the information processing system according to the second embodiment.

In Fig. 4, a united monitoring organization 400 includes the common-electronic-watermark extracting apparatus 205, corresponding to the common-electronic-watermark embedding apparatus 105, and the type-A to type-D electronic-watermark extracting apparatuses 206 to 209, corresponding to the type-A to type-D electronic-watermark embedding apparatuses 106 to 109 which employ the electronic-watermark methods unique to the organizations. A network 210 connects to the organizations 301 to 304, although they are not shown in Fig. 4. Instead of the organizations 301 to 304, the organizations 101 to 104 may be connected to the network 210.

An electronic-watermark extracting procedure to be executed in Fig. 4 will be described below.

09537877.032900
The organization 400 monitors data distributed or used in the network 210. If data which seems to be an
5 illegitimate copy is found or reported on the network, the organization 400 extracts information embedded by the common electronic-watermark method, by the use of the common-electronic-watermark extracting apparatus 205. With this operation, the organization which embedded the information
10 or the used method is identified. Then, various types of embedded information is extracted by the use of the extracting apparatus which employs the electronic-watermark method unique to the identified organization.

15 In the system according to the present embodiment, only the united monitoring organization can monitor illegitimate copying. Such a united monitoring organization can be implemented if a finite number of electronic-watermark methods unique to organizations are used. Since the electronic-watermark method unique to each organization is
20 identified by the common electronic-watermark method, it is not necessary to check an electronic watermark with the electronic-watermark method unique to each organization by trial and error, and therefore the system is efficient.

The united monitoring organization does not need to
25 have the electronic-watermark methods unique to all

organizations from the beginning. When the used embedding organization is identified by electronic-watermark information obtained by the common electronic-watermark method, it is possible that the united monitoring organization asks the embedding organization to send the extracting means employing the electronic-watermark method unique to the organization and its key.

(Third embodiment)

Fig. 5 shows a portion related to electronic-watermark extracting corresponding to the electronic-watermark embedding shown in Fig. 1 or Fig. 3.

In Fig. 5, organizations 501 to 504 have the common-electronic-watermark extracting apparatuses 205, corresponding to the common-electronic-watermark embedding apparatus 105, and the type-A to type-D electronic-watermark extracting apparatuses 206 to 209, corresponding to the type-A to type-D embedding apparatuses 106 to 109 employing the electronic-watermark methods unique to the organizations, respectively.

An electronic-watermark extracting procedure to be executed in Fig. 5 will be described below.

Each of the organizations 501 to 504 monitors data distributed or used on the network 210. If data which seems to be an illegitimate copy is found or reported in the network, the organization extracts information embedded by

the common electronic-watermark method, by the use of the common-electronic-watermark extracting apparatus 205. With this operation, the organization which embedded the information or the used method is identified. When it is determined that the organization employs the used method, it extracts information by the electronic-watermark extracting apparatus unique to the organization. When it is determined that another organization employs the used method, a notice is sent to the organization or the obtained information is discarded, according to conditions.

In the system according to the present embodiment, illegitimate copying can be monitored without having a united monitoring organization. This system can be applied to either of the embedding systems shown in Fig. 1 and Fig. 3. It is also clear that the extracting systems shown in Fig. 2 and Fig. 4 can be applied to either of the embedding systems shown in Fig. 1 and Fig. 3.

The system shown in Fig. 5 can be combined with that shown in Fig. 2 and that shown in Fig. 4. When the organization 200 according to the first embodiment shown in Fig. 2 has all of the type-A to type-D electronic-watermark extracting apparatuses as the organization 400 according to the second embodiment, and the organizations 201 and 202 have the common-electronic-watermark extracting apparatuses 205 in the same way as in the third embodiment, for example,

the organizations 203 and 204, which do not have the common-electronic-watermark extracting apparatus 205, execute the same processing as in the first embodiment, and the organizations 200, 210, and 202 can extract electronic-watermark information by the use of the common-electronic-watermark extracting apparatuses 205 within their organizations as in the second and third embodiments.

With the above cases being included, the present invention includes all techniques in which the common-electronic-watermark method having a high robustness and an electronic-watermark method unique to each organization are used according to conditions.

(Fourth embodiment)

In the embedding systems shown in Fig. 1 and Fig. 3, it is possible that each organization has the electronic-watermark extracting apparatus corresponding to the electronic-watermark embedding apparatus and an electronic-watermark extracting check is performed before electronic-watermark embedding.

This configuration can be applied to the first embodiment, the second embodiment, and a combination thereof. A fourth embodiment will be described below by referring to Fig. 6 with the embodiment shown in Fig. 3 being taken as an example.

In Fig. 6, a common-electronic-watermark embedding

organization 600 includes the common-electronic-watermark embedding apparatus 105 and the corresponding common-electronic-watermark extracting apparatus 205.

Organizations 601 to 604 have the type-A to type-D

- 5 electronic-watermark embedding apparatuses 106 to 109 employing the electronic-watermark methods unique to the organizations and the corresponding the type-A to type-D electronic-watermark extracting apparatuses 206 to 209.

- Each of the organizations 601 to 604 registers a
10 copyrighted material at the organization 600 and asks it to embed information by the use of the common-electronic-watermark embedding apparatus 105. The organization 600 checks whether the copyrighted material is not an illegitimate copy by the use of the common-electronic-
15 watermark extracting apparatus 205 before using the common-electronic-watermark embedding apparatus 105. When it is determined by the common-electronic-watermark extracting apparatus 205 that the common electronic watermark has been embedded in the copyrighted material, the organization 600
20 asks the embedding-request-source organization or the organization identified by the electronic-watermark information if there is no problem. When there is no problem, the organization 600 sends back predetermined information to the embedding-request-source organization by
25 the common-electronic-watermark embedding apparatus 105.

00537877.032900

The embedding-request-source organization embeds various types of information by the use of the electronic-watermark embedding apparatus, one of the apparatuses 106 to 109.

According to the system of the present embodiment,
5 electronic-watermark overwriting caused by an illegitimate report of a requester can be prevented. In addition, an efficient system is implemented because an electronic-watermark embedding organization and an electronic-watermark extracting organization are integrated as a unit.

10 A recording medium according to another embodiment of the present invention will be described below.

09537877.032900
15 The present invention is not limited to cases in which the systems and the apparatuses described in the above embodiments are combined. The present invention also includes cases in which a software program code for implementing each of the above embodiments is sent to the systems or the computers (CPUs or MPUs) of the apparatuses and the systems or the computers of the apparatuses operate the above-described various devices according to the program
20 code to implement each of the above embodiments.

In these cases, the program code of the software itself implements the functions of the above embodiments. Therefore, the present invention includes the program code itself, and means for sending the program code to a computer,
25 specifically, a recording medium for storing the program

code.

As recording media for storing the program code, semiconductor memories such as ROMs and RAMs, floppy disks, hard disks, optical disks, magneto-optical disks, CD-ROMs, magnetic tape, and non-volatile memory cards can be used.

The present invention includes the program code not only in cases in which the computers control various devices only according to the sent program code to implement the functions of the above-described embodiments, but also in cases in which the program code implements the above-described embodiments together with the operating systems operating on the computers or with other application software programs.

The present invention also includes a case in which a program code is stored in a memory provided for a function extending board or a function extending unit connected to a computer; a CPU provided for the function extending board or the function extending unit executes a part or the whole of actual processing; and the above-described embodiments are implemented by the processing.

As described above, according to the above embodiments, even in a system which uses different electronic-watermark methods, a monitoring organization efficiently monitors illegitimate copying without having many electronic-watermark embedding apparatuses and many electronic-

watermark extracting apparatuses. Improved safety is provided even in a case in which an electronic watermark is not found, as compared with a case in which each electronic-watermark method is used alone.

09537877.032900

WHAT IS CLAIMED IS:

1. An information processing system in which a plurality of information processing apparatuses are connected through a network, at least one of the plurality of information processing apparatuses comprising:

first adding means for adding first additional information to input information by a first adding method;
and

second adding means for adding second additional information to the input information by a second adding method,

wherein the first adding method has a higher robustness than the second adding method.

2. An information processing system according to Claim 1, further comprising communication means for communicating among the plurality of information processing apparatuses when said first adding means and said second adding means are provided for different information processing apparatuses.

3. An information processing system according to Claim 1, wherein the first additional information can be used for identifying the second adding method.

09537877.032900

4. An information processing system according to Claim 1, wherein the first additional information can be used for identifying each information processing apparatus on the network.

5. An information processing system according to Claim 1, wherein the second adding method is different from the first adding method.

6. An information processing system according to Claim 1, wherein the second additional information is unlikely to reduce the quality of the input information or is information which people are unlikely to perceive.

7. An information processing system according to Claim 1, wherein the second additional information is larger in amount than the first additional information.

8. An information processing system according to Claim 1, wherein the second adding method is the same as the first adding method.

9. An information processing system according to Claim 1, wherein the first adding method uses confidential

09537877-032900

information common to the plurality of information processing apparatuses.

10. An information processing system according to Claim 9, wherein the confidential information is the position of the first additional information or the amount of change against the first additional information.

11. An information processing system according to Claim 1, wherein the information processing apparatus further comprises first and second extracting means for extracting the first and second additional information, respectively, from the input information to which the first and second additional information has been added.

12. An information processing system according to Claim 11, wherein, before additional information is added to the input information by the use of said first or second adding means, whether additional information has been added to the input information is checked by the use of the first or second extracting means corresponding to the first or second adding means.

13. An information processing system in which a plurality of information processing apparatuses are

09537877.032900

connected through a network, at least one of the plurality of information processing apparatuses comprising:

first extracting means for extracting first additional information from input information by a first extracting method; and

second extracting means for extracting second additional information from the input information by a second extracting method identified by the extracted first additional information.

14. An information processing system according to Claim 13, further comprising communication means for communicating among the plurality of information processing apparatuses when said first adding means and said second adding means are provided for different information processing apparatuses.

15. An information processing system according to Claim 13, wherein the information processing apparatus further comprises determination means for determining that an attack has been made to the input information when only the first or the second additional information is extracted, and that the input information has no additional information when neither the first nor the second additional information is extracted.

09537877-032000

16. An information processing apparatus comprising:
first adding means for adding first additional
information to input information at a high robustness by a
first adding method; and
second adding means for adding second additional
information to the input information by a second adding
method.

17. An information processing apparatus according to
Claim 16, wherein the first additional information can be
used for identifying the second adding method.

18. An information processing apparatus according to
Claim 16, wherein the first additional information can be
used for identifying each information processing apparatus
on the network.

19. An information processing apparatus according to
Claim 16, wherein the second adding method is different from
the first adding method.

20. An information processing apparatus according to
Claim 16, wherein the second additional information is
unlikely to reduce the quality of the input information or

09537877.032900

is information which people are unlikely to perceive.

21. An information processing apparatus according to Claim 16, wherein the second additional information is larger in amount than the first additional information.

22. An information processing apparatus according to Claim 16, wherein the second adding method is the same as the first adding method.

23. An information processing apparatus according to Claim 16, wherein the first adding method uses confidential information common to the plurality of information processing apparatuses on the network.

24. An information processing apparatus according to Claim 23, wherein the confidential information is the position of the first additional information or the amount of change against the first additional information.

25. An information processing apparatus according to Claim 16, further comprising first and second extracting means for extracting the first and second additional information, respectively, from the input information to which the first and second additional information has been

09537877.032900

added.

26. An information processing apparatus according to Claim 25, wherein, before additional information is added to the input information by the use of said first or second adding means, whether additional information has been added to the input information is checked by the use of the first or second extracting means corresponding to the first or second adding means.

27. An information processing apparatus comprising:
first extracting means for extracting first additional information from input information by a first extracting method; and

second extracting means for extracting second additional information from the input information by a second extracting method identified by the extracted first additional information.

28. An information processing apparatus according to Claim 27, further comprising determination means for determining that an attack has been made to the input information when only the first or the second additional information is extracted, and that the input information has no additional information when neither the first nor the

09537877.032900

second additional information is extracted.

29. An information processing method comprising:

a first adding step of adding first additional information to input information at a high robustness by a first adding method; and

a second adding step of adding second additional information to the input information by a second adding method.

30. An information processing method comprising:

a first extracting step of extracting first additional information from input information by a first extracting method; and

a second extracting step of extracting second additional information from the input information by a second extracting method.

31. An information processing method according to Claim 30, further comprising a determination step of determining that an attack has been made to the input information when only the first or the second additional information is extracted, and that the input information has no additional information when neither the first nor the second additional information is extracted.

0537077.032900

32. A computer-readable recording medium for storing a program, the program comprising:

a first adding step of adding first additional information to input information at a high robustness; and

a second adding step of adding second additional information to the input information.

33. A computer-readable recording medium for storing a program, the program comprising:

a first extracting step of extracting first additional information from input information;

an identifying step of identifying an extracting method by the extracted first additional information; and

a second extracting step of extracting second additional information from the input information by the identified extracting method.

09537677.032900

ABSTRACT OF THE DISCLOSURE

In an information processing system, monitoring organizations embed highly robust information corresponding to the organizations in distributed input information as electronic watermarks by the use of a common-electronic-watermark embedding apparatuses. Then, the organizations embed another information by the use of electronic-watermark embedding apparatuses employing electronic-watermark methods unique to the organizations. When a predetermined monitoring organization finds illegitimately copied data on a network, it extracts information embedded by either of the above-described common-electronic-watermark embedding apparatuses, by the use of a common-electronic-watermark extracting apparatus. With this operation, the organization which has performed embedding is identified. The data is sent to the identified organization. The organization extracts various types of embedded information by the use of an extracting apparatus unique to the organization. Therefore, each organization just needs to manage only an electronic-watermark embedding apparatus and an electronic-watermark extracting apparatus employing a method unique to the organization, without having embedding apparatuses and extracting apparatuses employing many methods.

09537877-032900

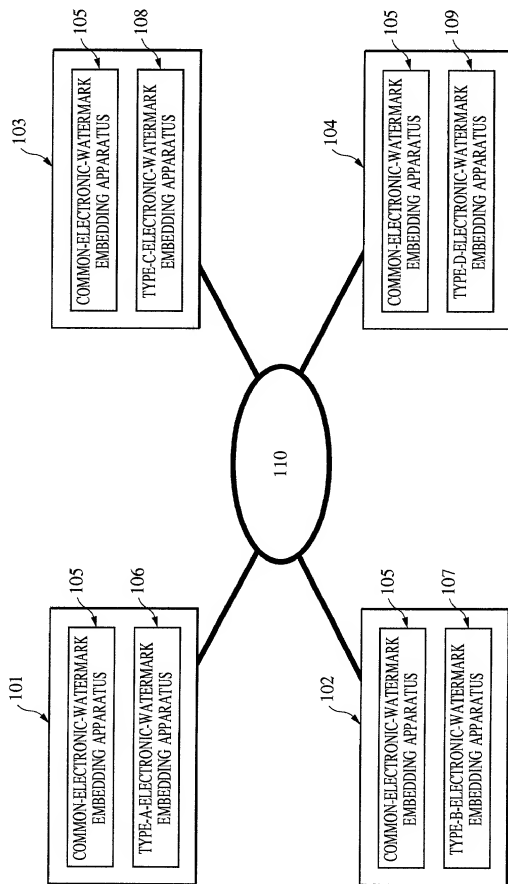


FIG. 1

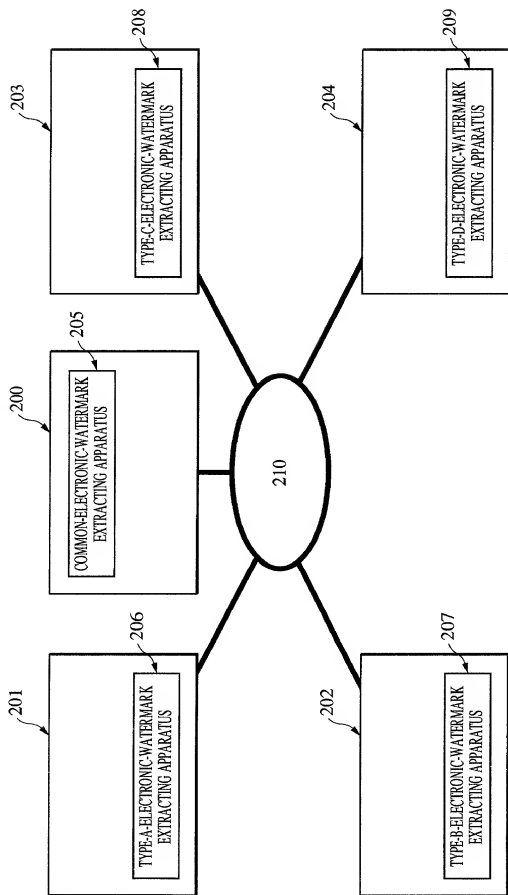


FIG. 2

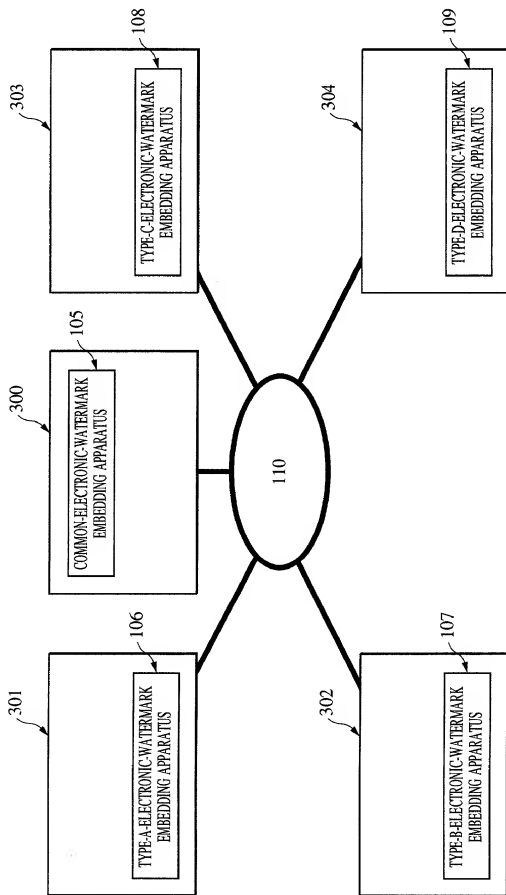


FIG. 3

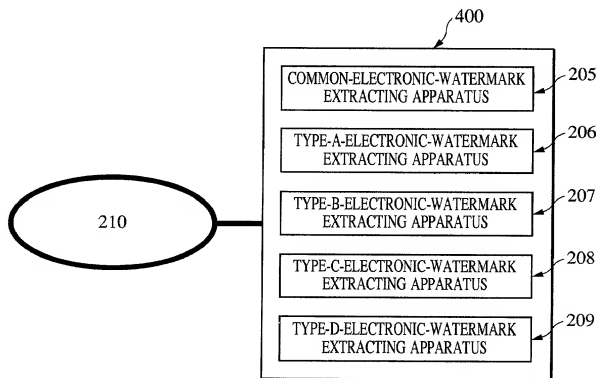


FIG. 4

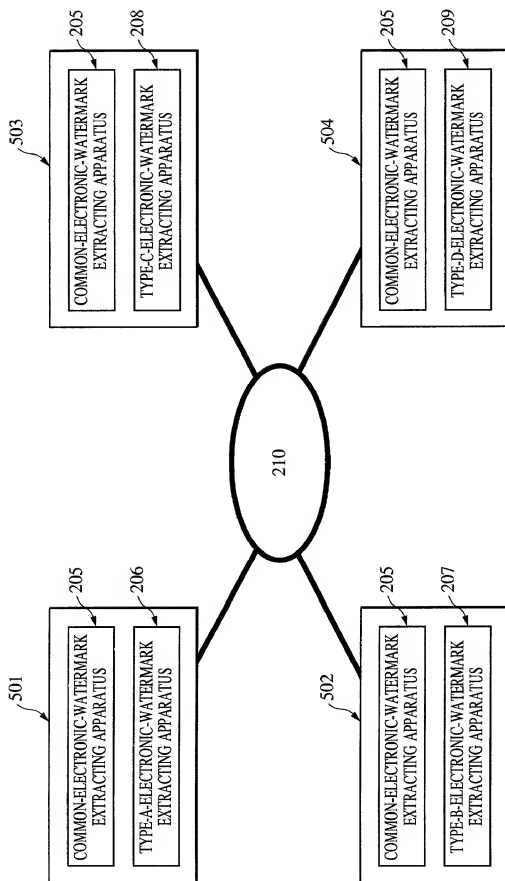


FIG. 5

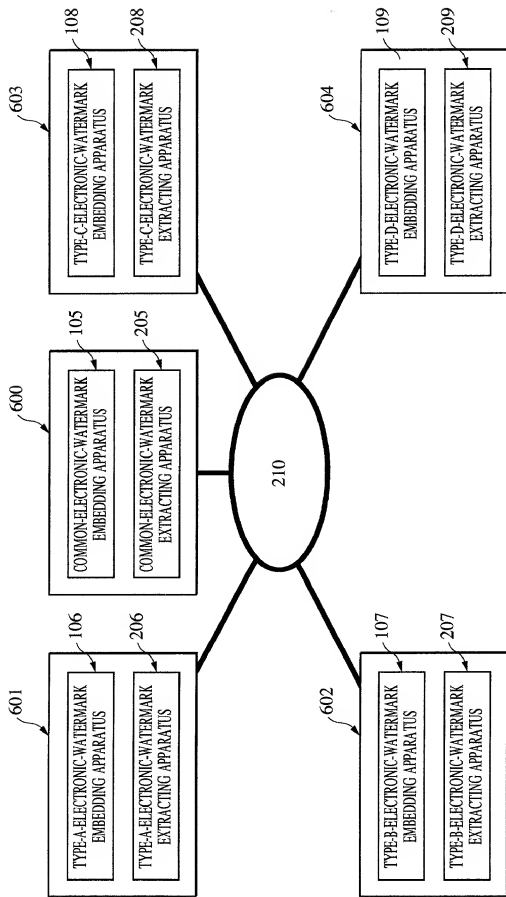


FIG. 6

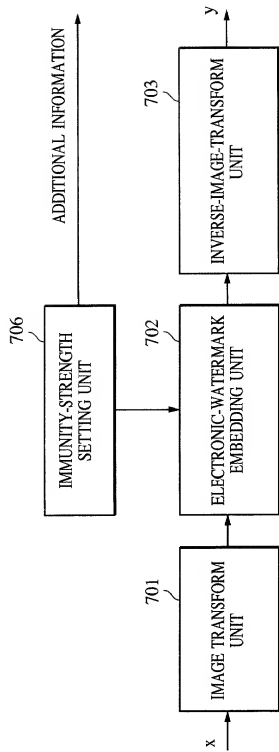


FIG. 7A

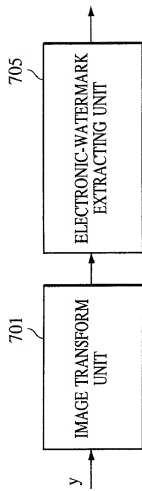


FIG. 7B

**COMBINED DECLARATION AND POWER OF ATTORNEY
FOR PATENT APPLICATION**

(Page 1)

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled INFORMATION PROCESSING SYSTEM, INFORMATION PROCESSING APPARATUS, AND COMPUTER-READABLE RECORDING MEDIUM the specification of which ☒ is attached hereto ☐ was filed on _____ as United States Application No. or PCT International Application No. _____ (if applicable), and was amended on _____

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR §1.56.

I hereby claim foreign priority benefits under 35 U.S.C. §119(a)-(d) or §365(b), of any foreign application(s) for patent or inventor's certificate, or §365(a) of any PCT international application which designates at least one country other than the United States, listed below and have also identified below any foreign application for patent or inventor's certificate, or PCT international application having a filing date before that of the application on which priority is claimed:

Country	Application No.	Filed (Day/Mo./Yr.)	(Yes/No) Priority Claimed
JAPAN	11-093000	31 MARCH 1999	Yes

I hereby claim the benefit under 35 U.S.C. § 120 of any United States application(s), or § 365(c) of any PCT international application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT international application in the manner provided by the first paragraph of 35 U.S.C. § 112, I acknowledge the duty to disclose information which is material to patentability as defined in 37 C.F.R. § 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application.

Application No.	Filed (Day/Mo./Yr.)	Status (Patented, Pending, Abandoned)

I hereby appoint the practitioners associated with the firm and Customer Number provided below to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith, and direct that all correspondence be addressed to the address associated with that Customer Number:

FITZPATRICK, CELLA, HARPER & SCINTO
Customer Number: 05514

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of Sole or First Inventor Keiichi IWAMURA
Inventor's signature _____
Date _____ Citizen/Subject of Japan
Residence 4-29-2-405, Futaba-cho, Minami-ku, Yokohama-shi, Kanagawa-ken, Japan
Post Office Address c/o CANON KABUSHIKI KAISHA, 30-2, Shimomaruko 3-chome, Ohta-ku, Tokyo, Japan

BLKlcmv